CLAIMS

What is claimed is:

1. A method of protecting an asset of an information and/or physical type, comprising the step of:

providing processor-based physical asset protection, providing processor-based information asset protection, and integrating said processor-based physical asset protection and said processor-based information asset protection in a hosted environment.

2. The method of claim 1, said integrating step comprising providing, maintaining and operating a software application that integrates said physical asset protection and said information asset protection in said hosted environment in accordance with user instructions.

3. The method of claim 1, further comprising the steps of:

registering a user by storing user information;

authenticating a user by comparing at least one user characteristic from said user information with a third-party database;

comparing a current asset use pattern with a historical asset use pattern for said user to detect anomalous usage;

updating said historical use pattern on the basis of said current use pattern;

taking a corrective action, wherein a first corrective action is taken if said authenticating step generates a non-authenticated user output and a second corrective action is taken if anomalous usage is detected during said comparing step; and

wherein said authenticating and comparing steps provide physical asset protection and information asset protection and are performed in said hosted environment.

4. The method of claim 3, wherein said corrective action comprises at least one of triggering an alert to a third party, providing a report to an asset manager, logging said non-authenticated user output, disabling network logons, disconnecting other users from said network, and disabling physical access to said asset.

5. The method of claim 1, further comprising the steps of:

registering a visitor by providing initial visitor information;

comparing said initial visitor information with a third-party database to determine if said registered visitor is entitled to access to said asset; and

receiving said registered visitor in an authentication area;

checking a match of said registered visitor with a physical entity;

regulating entry on the basis of said checking and comparing steps, wherein said registered visitor is denied access if said registered visitor does not match said physical entity, or said comparing step indicates that said visitor does not have access to said asset; and

wherein at least one of said comparing step, said receiving step and said checking step provide physical asset protection and information asset protection.

6. The method of claim 5, further comprising one of triggering an alert or a report to an asset manager, logging said non-authenticated user output, disabling network logons, disconnecting other users from said network, and disabling physical access to said asset when said visitor is denied access.

7. The method of claim 5, wherein one of said receiving step and said comparing step comprises applying biometrics to control access for said user.

8. The method of claim 7, wherein said biometrics comprises one of scanning and testing a target tissue of said visitor's body.

9. The method of claim 1, wherein said physical asset protection comprises securing ingress and egress areas for a location protected by a physical barrier.

10. The method of claim 1, further comprising providing an engineering service by collecting and analyzing access information in a data/event repository in said hosted environment that is integrated with an asset environment to perform one of security asset tracking, employee and visitor tracking, physical intrusion monitoring, and network access control and intrusion monitoring.

11. The method of claim 1, further comprising periodically reviewing security information in an access database of said hosted environment to substantially eliminate fraudulent use of said database.

12. A system for protecting an asset, comprising:

a physical asset protection module that provides physical protection for said asset;

an information asset protection module that provides information security protection for said asset; and

an integrator that performs an integration of said physical asset protection module and said information asset protection module, wherein said system is one of in a hosted environment and at said asset.

13. The asset protection system of claim 12, further comprising a user tracking system that authenticates a user as a registered user and provides physical access and information access to said asset in accordance with historical use patterns of said user for said asset, wherein said user tracking system updates said historical use patterns in accordance with a current use pattern of said user.

14. The asset protection system of claim 13, said historical use patterns comprising at least one of frequency, type and time duration.

15. The asset protection system of claim 12, further comprising a visitor tracking system that authenticates a registered visitor that has not been barred from accessing said asset, and allows access in accordance with reception authentication process.

16. The asset protection system of claim 15, further comprising a biometrics authentication subsystem that uses physical data of said visitor to allow said access.

17. The asset protection system of claim 16, wherein said physical data comprises a test data portion of said visitor's body.

18. The asset protection system of claim 12, further comprising a sub-module in said hosted environment, said submodule performing at least one of security asset tracking, employee and visitor tracking, physical intrusion monitoring, network access control and continual monitoring of an access database to substantially eliminate fraudulent use and entry.

19. The asset protection system of claim 12, wherein said integration is performed in response to an instruction to develop, maintain and operate a computer application to protect said asset.

20. A method of providing asset security protection, comprising:

transmitting a first signal to a hosted environment, said first signal comprising user registration characteristics; and

receiving a second signal from said hosted environment indicative of asset access, wherein protection of physical and information characteristics of said asset is integrated in said hosted environment.

21. The method of claim 20, wherein said transmitting step comprises:

providing user registration information to said hosted environment; and

processing at said hosted environment said user information to generate said second signal.

22. The method of claim 20, wherein said receiving step comprises receiving an access decision from said hosted environment, said decision being in accordance with biometrics of a user.

23. The method of claim 20, further comprising comparing said user information to a third-party database to generate an authentication output as said second signal.

24. The method of claim 1, further comprising the steps of:

entering credentials of a user into an access database in said hosted environment to enroll said user; and

outputting an identification object in accordance with said credentials, wherein unauthorized access is denied by said hosted environment.

25. The method of claim 23, said entering step comprising the steps of:

providing an authorized operator with permission to at least one of alter and append said access database;

obtaining a biometric from said user and searching for said biometric in said access database to generate a search result, wherein said biometric and credential data is added to said access database if said search result indicates an absence of said biometric, and if said search result indicates a presence of said biometric in said access database, one of verifying said credential data if said user is authentic and denying access to said user if said user is not authentic, in accordance with said biometric;

denying access to said user if said user appears in a barred user database;

determining if a photo of said user is in said hosted environment, wherein a digital image is imported to generate said photo if said photo is not present in said hosted environment;

verifying that said photo represents said new user;

providing additional user information and user access privileges to said hosted environment; and

generating said identification object having a predetermined layout, said identification object comprising an encrypted three-dimensional barcode in accordance with said biometric and said credential data.

26. The method of claim 23, said outputting step comprising the steps of:

receiving said identification object from said hosted environment and producing a copy of said identification object;

said user verifying integrity of said biometric, said photo and said credentials; and

distributing said identification object to said user.

27. The method of claim 25, wherein said identification object is produced by printing an identification badge.

28. The method of claim 24, wherein said biometric comprises a scan of a biological target tissue.

29. The method of claim 27, wherein said target tissue comprises at least one of finger, hand and eye parameter.